

**Introduced by Senator Johnston**

February 18, 1998

---

An act to amend Section 502 of the Penal Code, relating to computer crimes.

LEGISLATIVE COUNSEL'S DIGEST

SB 1734, as introduced, Johnston. Computer crimes: employees.

Existing law prohibits various computer crimes, including the fraudulent destruction of computer systems, programs, networks, or data, the theft of data or materials, the illegal provision or disruption of access, or the introduction of computer viruses. Existing law also provides that these provisions do not apply to an employee who accesses his or her employer's computer system, network, programs, or data when acting within the scope of his or her employment.

This bill would clarify that an employee is acting within the scope of his or her employment only when he or she accesses the system, network, program, or data in order to perform duties that are within the express or implied authority granted by the employer with reference to the employee's work assignment.

Vote: majority. Appropriation: no. Fiscal committee: no. State-mandated local program: no.

*The people of the State of California do enact as follows:*

1 SECTION 1. Section 502 of the Penal Code is  
2 amended to read:

1 502. (a) It is the intent of the Legislature in enacting  
2 this section to expand the degree of protection afforded  
3 to individuals, businesses, and governmental agencies  
4 from tampering, interference, damage, and  
5 unauthorized access to lawfully created computer data  
6 and computer systems. The Legislature finds and  
7 declares that the proliferation of computer technology  
8 has resulted in a concomitant proliferation of computer  
9 crime and other forms of unauthorized access to  
10 computers, computer systems, and computer data.

11 The Legislature further finds and declares that  
12 protection of the integrity of all types and forms of  
13 lawfully created computers, computer systems, and  
14 computer data is vital to the protection of the privacy of  
15 individuals as well as to the well-being of financial  
16 institutions, business concerns, governmental agencies,  
17 and others within this state that lawfully utilize those  
18 computers, computer systems, and data.

19 (b) For the purposes of this section, the following  
20 terms have the following meanings:

21 (1) "Access" means to gain entry to, instruct, or  
22 communicate with the logical, arithmetical, or memory  
23 function resources of a computer, computer system, or  
24 computer network.

25 (2) "Computer network" means any system which  
26 provides communications between one or more  
27 computer systems and input/output devices including,  
28 but not limited to, display terminals and printers  
29 connected by telecommunication facilities.

30 (3) "Computer program or software" means a set of  
31 instructions or statements, and related data, that when  
32 executed in actual or modified form, cause a computer,  
33 computer system, or computer network to perform  
34 specified functions.

35 (4) "Computer services" includes, but is not limited to,  
36 computer time, data processing, or storage functions, or  
37 other uses of a computer, computer system, or computer  
38 network.

39 (5) "Computer system" means a device or collection  
40 of devices, including support devices and excluding



1 calculators which are not programmable and capable of  
2 being used in conjunction with external files, one or more  
3 of which contain computer programs, electronic  
4 instructions, input data, and output data, that performs  
5 functions including, but not limited to, logic, arithmetic,  
6 data storage and retrieval, communication, and control.

7 (6) “Data” means a representation of information,  
8 knowledge, facts, concepts, computer software,  
9 computer programs or instructions. Data may be in any  
10 form, in storage media, or as stored in the memory of the  
11 computer or in transit or presented on a display device.

12 (7) “Supporting documentation” includes, but is not  
13 limited to, all information, in any form, pertaining to the  
14 design, construction, classification, implementation, use,  
15 or modification of a computer, computer system,  
16 computer network, computer program, or computer  
17 software, which information is not generally available to  
18 the public and is necessary for the operation of a  
19 computer, computer system, computer network,  
20 computer program, or computer software.

21 (8) “Injury” means any alteration, deletion, damage,  
22 or destruction of a computer system, computer network,  
23 computer program, or data caused by the access.

24 (9) “Victim expenditure” means any expenditure  
25 reasonably and necessarily incurred by the owner or  
26 lessee to verify that a computer system, computer  
27 network, computer program, or data was or was not  
28 altered, deleted, damaged, or destroyed by the access.

29 (10) “Computer contaminant” means any set of  
30 computer instructions that are designed to modify,  
31 damage, destroy, record, or transmit information within  
32 a computer, computer system, or computer network  
33 without the intent or permission of the owner of the  
34 information. They include, but are not limited to, a group  
35 of computer instructions commonly called viruses or  
36 worms, which are self-replicating or self-propagating and  
37 are designed to contaminate other computer programs or  
38 computer data, consume computer resources, modify,  
39 destroy, record, or transmit data, or in some other fashion

1 usurp the normal operation of the computer, computer  
2 system, or computer network.

3 (c) Except as provided in subdivision (h), any person  
4 who commits any of the following acts is guilty of a public  
5 offense:

6 (1) Knowingly accesses and without permission alters,  
7 damages, deletes, destroys, or otherwise uses any data,  
8 computer, computer system, or computer network in  
9 order to either (A) devise or execute any scheme or  
10 artifice to defraud, deceive, or extort, or (B) wrongfully  
11 control or obtain money, property, or data.

12 (2) Knowingly accesses and without permission takes,  
13 copies, or makes use of any data from a computer,  
14 computer system, or computer network, or takes or  
15 copies any supporting documentation, whether existing  
16 or residing internal or external to a computer, computer  
17 system, or computer network.

18 (3) Knowingly and without permission uses or causes  
19 to be used computer services.

20 (4) Knowingly accesses and without permission adds,  
21 alters, damages, deletes, or destroys any data, computer  
22 software, or computer programs which reside or exist  
23 internal or external to a computer, computer system, or  
24 computer network.

25 (5) Knowingly and without permission disrupts or  
26 causes the disruption of computer services or denies or  
27 causes the denial of computer services to an authorized  
28 user of a computer, computer system, or computer  
29 network.

30 (6) Knowingly and without permission provides or  
31 assists in providing a means of accessing a computer,  
32 computer system, or computer network in violation of  
33 this section.

34 (7) Knowingly and without permission accesses or  
35 causes to be accessed any computer, computer system, or  
36 computer network.

37 (8) Knowingly introduces any computer contaminant  
38 into any computer, computer system, or computer  
39 network.



1 (d) (1) Any person who violates any of the provisions  
2 of paragraph (1), (2), (4), or (5) of subdivision (c) is  
3 punishable by a fine not exceeding ten thousand dollars  
4 (\$10,000), or by imprisonment in the state prison for 16  
5 months, or two or three years, or by both that fine and  
6 imprisonment, or by a fine not exceeding five thousand  
7 dollars (\$5,000), or by imprisonment in the county jail not  
8 exceeding one year, or by both that fine and  
9 imprisonment.

10 (2) Any person who violates paragraph (3) of  
11 subdivision (c) is punishable as follows:

12 (A) For the first violation which does not result in  
13 injury, and where the value of the computer services used  
14 does not exceed four hundred dollars (\$400), by a fine not  
15 exceeding five thousand dollars (\$5,000), or by  
16 imprisonment in the county jail not exceeding one year,  
17 or by both that fine and imprisonment.

18 (B) For any violation which results in a victim  
19 expenditure in an amount greater than five thousand  
20 dollars (\$5,000) or in an injury, or if the value of the  
21 computer services used exceeds four hundred dollars  
22 (\$400), or for any second or subsequent violation, by a  
23 fine not exceeding ten thousand dollars (\$10,000), or by  
24 imprisonment in the state prison for 16 months, or two or  
25 three years, or by both that fine and imprisonment, or by  
26 a fine not exceeding five thousand dollars (\$5,000), or by  
27 imprisonment in the county jail not exceeding one year,  
28 or by both that fine and imprisonment.

29 (3) Any person who violates paragraph (6), (7), or (8)  
30 of subdivision (c) is punishable as follows:

31 (A) For a first violation which does not result in injury,  
32 an infraction punishable by a fine not exceeding two  
33 hundred fifty dollars (\$250).

34 (B) For any violation which results in a victim  
35 expenditure in an amount not greater than five thousand  
36 dollars (\$5,000), or for a second or subsequent violation,  
37 by a fine not exceeding five thousand dollars (\$5,000), or  
38 by imprisonment in the county jail not exceeding one  
39 year, or by both that fine and imprisonment.

1 (C) For any violation which results in a victim  
2 expenditure in an amount greater than five thousand  
3 dollars (\$5,000), by a fine not exceeding ten thousand  
4 dollars (\$10,000), or by imprisonment in the state prison  
5 for 16 months, or two or three years, or by both that fine  
6 and imprisonment, or by a fine not exceeding five  
7 thousand dollars (\$5,000), or by imprisonment in the  
8 county jail not exceeding one year, or by both that fine  
9 and imprisonment.

10 (e) (1) In addition to any other civil remedy  
11 available, the owner or lessee of the computer, computer  
12 system, computer network, computer program, or data  
13 may bring a civil action against any person convicted  
14 under this section for compensatory damages, including  
15 any expenditure reasonably and necessarily incurred by  
16 the owner or lessee to verify that a computer system,  
17 computer network, computer program, or data was or  
18 was not altered, damaged, or deleted by the access. For  
19 the purposes of actions authorized by this subdivision, the  
20 conduct of an unemancipated minor shall be imputed to  
21 the parent or legal guardian having control or custody of  
22 the minor, pursuant to the provisions of Section 1714.1 of  
23 the Civil Code.

24 (2) In any action brought pursuant to this subdivision  
25 the court may award reasonable attorney's fees to a  
26 prevailing party.

27 (3) A community college, state university, or  
28 academic institution accredited in this state is required to  
29 include computer-related crimes as a specific violation of  
30 college or university student conduct policies and  
31 regulations that may subject a student to disciplinary  
32 sanctions up to and including dismissal from the academic  
33 institution. This paragraph shall not apply to the  
34 University of California unless the Board of Regents  
35 adopts a resolution to that effect.

36 (f) This section shall not be construed to preclude the  
37 applicability of any other provision of the criminal law of  
38 this state which applies or may apply to any transaction,  
39 nor shall it make illegal any employee labor relations



1 activities that are within the scope and protection of state  
2 or federal labor laws.

3 (g) Any computer, computer system, computer  
4 network, or any software or data, owned by the  
5 defendant, which is used during the commission of any  
6 public offense described in subdivision (c) or any  
7 computer, owned by the defendant, which is used as a  
8 repository for the storage of software or data illegally  
9 obtained in violation of subdivision (c) shall be subject to  
10 forfeiture, as specified in Section 502.01.

11 (h) (1) Subdivision (c) does not apply to any person  
12 who accesses his or her employer's computer system,  
13 computer network, computer program, or data when  
14 acting within the scope of his or her lawful employment.  
15 *An employee is acting within the scope of his or her*  
16 *employment only when he or she accesses his or her*  
17 *employer's computer system, network, programs, or data*  
18 *to perform duties that are within the express or implied*  
19 *authority granted by the employer to that employee for*  
20 *the performance of his or her work assignment.*

21 (2) Paragraph (3) of subdivision (c) does not apply to  
22 any employee who accesses or uses his or her employer's  
23 computer system, computer network, computer  
24 program, or data when acting outside the scope of his or  
25 her lawful employment, so long as the employee's  
26 activities do not cause an injury, as defined in paragraph  
27 (8) of subdivision (b), to the employer or another, or so  
28 long as the value of supplies and computer services, as  
29 defined in paragraph (4) of subdivision (b), which are  
30 used do not exceed an accumulated total of one hundred  
31 dollars (\$100).

32 (i) No activity exempted from prosecution under  
33 paragraph (2) of subdivision (h) which incidentally  
34 violates paragraph (2), (4), or (7) of subdivision (c) shall  
35 be prosecuted under those paragraphs.

36 (j) For purposes of bringing a civil or a criminal action  
37 under this section, a person who causes, by any means, the  
38 access of a computer, computer system, or computer  
39 network in one jurisdiction from another jurisdiction is  
40 deemed to have personally accessed the computer,

1 computer system, or computer network in each  
2 jurisdiction.

3 (k) In determining the terms and conditions  
4 applicable to a person convicted of a violation of this  
5 section the court shall consider the following:

6 (1) The court shall consider prohibitions on access to  
7 and use of computers.

8 (2) Except as otherwise required by law, the court  
9 shall consider alternate sentencing, including community  
10 service, if the defendant shows remorse and recognition  
11 of the wrongdoing, and an inclination not to repeat the  
12 offense.

